WHAT IS CLAIMED IS:

1. A method for detecting hostile software in a computer system comprising:

storing a representation of configuration data associated with an operating system for the computer system obtained at a first time;

comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time; and

if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time, automatically performing at least one remedial measure in response to the deviation detected.

2. The method of claim 1 wherein the configuration data relates to identification of executable code installed in the computer system.

3. The method of claim 1 wherein the configuration data relates to identification of a command line for invoking executable code associated with a particular file extension.

4. The method of claim 1 wherein the configuration data is obtained from a registry maintained by the operating system.

5. The method of claim 4 wherein the configuration data obtained from at least one key associated with the registry.

6. The method of claim 1 wherein the configuration data is obtained from a file stored in the computer system.

7. The method of claim 1 wherein the stored representation of configuration data is encoded prior to being stored.

8. The method of claim 1 wherein the configuration data is compared to a predefined value.

9. The method of claim 1 wherein the configuration data is checked for addition of data.

10. The method of claim 1 wherein the configuration data is checked for removal of data.

11. The method of claim 1 wherein the at least one remedial measure comprises determining a storage location associated with suspected executable code in the computer system.

12. The method of claim 1 wherein the at least one remedial measure comprises determining whether suspected executable code is currently executing.

13. The method of claim 12 wherein the at least one remedial measure further comprises terminating execution of the suspected executable code.

14. The method of claim 13, wherein the suspected executable code does not receive notification prior to being terminated.

15. The method of claim 1 wherein the at least one remedial measure comprises moving suspected executable code to a specified storage location for later evaluation.

16. The method of claim 1 wherein the at least one remedial measure comprises altering configuration data associated with the operating system to reflect the stored representation of the configuration data.

17. The method of claim 1 wherein the operating system is a Windows-based operating system.

18. The method of claim 1 wherein the operating system is a Linux-based operating system.

19. A computer system capable of detecting hostile software comprising:

a processing unit capable of being controlled by an operating system;

a storage unit coupled to the processing unit, the storage unit capable of storing a representation of configuration data associated with the operating system obtained at a first time;

wherein the processing unit is capable of comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system obtained at a second time and, if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time, automatically performing at least one remedial measure in response to the deviation detected.

20. A system for detecting hostile software in a computer system comprising:

means for storing a representation of configuration data associated with an operating system for the computer system obtained at a first time;

means for comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time; and

means for automatically performing at least one remedial measure in response to the deviation detected, if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time.

21. An article of manufacture comprising:

a computer usable medium having computer readable program code means embodied therein for causing hostile software to be detected in a computer system, the computer readable program code means in said article of manufacture comprising:

computer readable program code means for causing a computer to store a representation of configuration data associated with an operating system for the computer system obtained at a first time;

computer readable program code means for causing the computer to compare the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time; and

computer readable program code means for causing the computer to automatically perform at least one remedial measure in response to the deviation detected, if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time.